CLAIMS

What is claimed is:

1. A method of transporting electronic data for secure storage on an archive server, comprising the steps of:

providing at least one client workstation having a Web browser running thereon;

accessing the Web browser from the client workstation and logging onto a qualified Web server;

providing account qualifier data to a software application residing on the Web server;

obtaining an encryption applet from the software application;

selecting an electronic data file to be encrypted;

encrypting said electronic data file and forming an encrypted data packet;

transferring said encrypted data packet to the archive server; and

destroying the encryption applet.

2. The method of claim 1, wherein the software application residing on the Web server is platform-independent.

3. The method of claim 1, further including the step of compressing the encrypted data packet prior to transferring the encrypted data packet to the archive server.

4. The method of claim 3, wherein the encryption applet includes a compression

program to compress the electronic data to form a compressed encrypted data packet.

5. The method of claim 1, wherein the encryption applet compiled by the software application is based on an encryption algorithm, and the encryption algorithm is changeable with respect to the software application.

6. The method of claim 1, further comprising the steps of:

providing a plurality of encryption algorithms;

selecting an encryption algorithm; and

compiling the encryption applet using the selected encryption algorithm.

7. The method of claim 6, wherein a user at the client workstation can select the encryption algorithm.

8. The method of claim 1, further including providing a plurality of client workstations, wherein at least two of the plurality of client workstations are coupled via a network.

9. The method of claim 8, wherein the archive server is coupled to at least one of the plurality of client workstations.

10. The method of claim 8, wherein the archive server is coupled to the network.

11. The method of claim 1, further comprising the step of assigning access permission to said encrypted data packet, wherein the access permission permits selective access to the electronic data files.

12. The method of claim 11, wherein access permission is assigned to a user having designated account qualifier data.

13. The method of claim 11, wherein said access permission permits hierarchal access to an electronic data file by a group of users.

14. The method of claim 1 wherein the encrypted data packet is transferred from the client workstation to the archive server by SSL protocol.

15. A method of retrieving encrypted electronic data stored on an archive server, comprising the steps of:

providing at least one encrypted data packet on the archive server;

providing at least one client workstation having a Web browser;

accessing the Web browser and logging onto a qualified Web server;

providing account qualifier data to as software application residing on the Web server;

selecting an encrypted data packet to be retrieved from the archive server;

obtaining a decryption applet from the application based on the original encryption algorithm of the encrypted data packet

transferring the decryption applet and the encrypted data packet to the client workstation; and

decrypting said encrypted data packet at the client workstation, whereby the electronic data is available to a user at the client workstation.

16. The method of claim 15, wherein the account qualifier data corresponds to at least one user.

17. The method of claim 15, wherein said encrypted data packet is compressed, and said decryption applet includes a decompression program to decompress the encrypted data packet.

18. The method of claim 15, wherein the software application residing on said Web server is platform-independent.

19. The method of claim 15, wherein the at least one client workstation comprises a plurality of client workstations.

20. The method of claim 15, wherein the at least two of the plurality of client workstations are coupled via a network.

21. The method of claim 15, wherein the archive server is coupled to the at least one client workstation.

22. The method of claim 20, wherein the archive server is coupled to the network.

23. The method of claim 15, wherein access permission is assigned to at least one encrypted data packet, wherein the access permission permits selective access to the electronic data files.

24. The method of claim 15, wherein the encrypted data packet is transferred from the to the archive server to the client workstation by SSL protocol.

25. A system for secure storage of electronic data on an archive server, comprising:

a plurality of client workstations, said plurality of client workstations having Web browsers running thereon;

a platform-independent software application residing on a Web server,

means for qualifying a authorization user of said software application;

means for encrypting an electronic file at said client workstations, said means comprising an encryption applet compiled by said software application which is transmitted to a user at one of said client workstations; said encryption applet operable to encrypt the electronic file to create an encrypted data packet;

means for transmitting said encrypted data packet to said archive server for secure storage;

means for retrieving said encrypted data packet from said archive server; and

means for decrypting said encrypted data packet, said means comprising obtaining a decryption applet from said software application, said decryption applet compiled by said software application based on the original encryption algorithm.

26. The system of claim 25, wherein said encryption applet includes a means to compress said encrypted data packet.

27. The system of claim 25, wherein said encryption applet includes a means to decompress a compressed encrypted data packet.

28. The system of claim 25, wherein the software application compiles the encryption applet using an encryption algorithm, and the encryption algorithm is changeable with respect to the application.

29. The system of claim 25, further comprising a means to select the encryption algorithm.

30. The system of claim 25, wherein two of the plurality of client workstations are coupled via a network.

31. The system of claim 25, wherein the archive server is coupled to at least one of the plurality of client workstations.

32. The system of claim 25, wherein the archive server is coupled to the network.

33. The system of claim 25, wherein access permission is assigned to said encrypted data packet, wherein said access permission permits selective access to the electronic data files.

34. The system of claim 33, wherein said access permission is assigned to a user having designated account qualifier data.

35. The system of claim 33, wherein said access permission permits hierarchal access to an electronic data file by a group of users.

36. The system of claim 34, wherein the means for transmitted the encrypted data packet from the client workstation to the archive server is by SSL protocol.

37. The system of claim 25, wherein the means for transmitted the encrypted data packet from the archive server is by SSL protocol.

40. The system according to claim 25, wherein said software application is accessed by account qualifier data.